Legislative Audit Division

State of Montana

Report to the Legislature

August 2004

Information System Audit

The University of Montana - Missoula Key Computer Application and General Controls Audit

This report provides information regarding key computer application and general controls relevant to The University of Montana - Missoula Banner computer application. The report contains three recommendations addressing:

- **Inadequate environmental controls**
- **Excessive physical access**
- **Distributed network security administration**

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

04DP-03

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator John Cobb	Representative Dee Brown
Senator Mike Cooney	Representative Tim Callahan
Senator Jim Elliott, Vice Chair	Representative Hal Jacobson
Senator John Esp	Representative John Musgrove
Senator Dan Harrington	Representative Jeff Pattison, Chair
Senator Corey Stapleton	Representative Rick Ripley

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

August 2004

The Legislative Audit Committee
of the Montana State Legislature:

This is the report of our information systems audit of the controls relating to the Banner computer system operated by The University of Montana - Missoula. We performed a limited review of general and application controls over the Banner system. This report contains three recommendations: physical and environmental security controls improvement, compliance with the Board of Regents policy requirement to designate an information security manager, and identification of network security issues and exposures and subsequent policy development. The University of Montana - Missoula's response to the audit report is contained at the end of the report.

We wish to express our appreciation to the staff of The University of Montana - Missoula for their cooperation and assistance.

Respectfully submitted,

(Signature on File)

Scott A. Seacat
Legislative Auditor

Room 160, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@state.mt.us

Legislative Audit Division

Information System Audit

The University of Montana - Missoula Key Computer Application and General Controls Audit

Members of the audit staff involved in this audit were Charles Nemec and Jessica Solem.

Table of Contents

Appointed and Administrative Officials

The University of Montana - Missoula	George Dennison, President The University of Montana - Missoula
	Dan Dwyer, Vice President Office of Research and Development
	Ray Ford, Associate Vice President Information Technology
	Steve Henry, Director Computing and Information Services
	Kathy Burgmeier, Director Internal Audit

Executive Summary

Executive Summary

Administration of The University of Montana (UM) - Missoula's information technology as it relates to the Banner application, is the responsibility of the Computing and Information Services (CIS) department. Financial aid, human resource, and financial data is processed using the Banner system. Banner is a commercial software application developed by SunGard Systems and Computer Technology Corporation (SCT) and is a product used by higher education entities for managing their business processes.

The network and its security provide the foundation for all systems and software applications and, therefore, is central to all of The UM - Missoula's business goals, requirements, and operations. CIS controls the network, including managing central equipment and operations. However, security for some aspects of the network is distributed among CIS and business process owners, because The UM - Missoula business process owners control and administer hardware, such as servers and desktops, residing on the network.

We audit selected The UM Banner processes approximately every two years to understand the control environment. The current audit scope is based on specific control testing requested by Legislative Audit Division Financial-Compliance staff and specific general controls testing determined relevant to the Banner application. We performed audit work on The UM – Missoula campus to meet three objectives: 1) to provide assurance over key Banner application controls identified by Financial-Compliance audit staff, 2) to evaluate the general controls environment where the Banner application resides, and 3) to review the security administration over the network environment and assess the security of selected workstations residing on the network.

Summary

The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office. The current report contains three recommendations addressing:

1. Inadequate environmental conditions created by the existence of water sources near Banner backup equipment, network equipment, and power cabling

2. Excessive physical access to the computer facility housing Banner backup and network equipment

3. Compliance with Board of Regents policy by identifying security issues and exposures and developing polices addressing those concerns and designating an information security manager

In addition to this report, we provided a technical memorandum to the Legislative Audit Division Financial-Compliance staff providing results of key Banner application control testing for consideration during financial audits.

Chapter I - Introduction and Background

Introduction and Background

Administration of The UM - Missoula's information technology as it relates to the Banner application, is the responsibility of the Computing and Information Services (CIS) department. Financial aid, human resource, and financial data is processed using the Banner system. Banner is a commercial software application developed by SunGard Systems and Computer Technology Corporation (SCT) and is a product used by higher education entities for managing their business processes.

The network and its security provide the foundation for all systems and software applications and, therefore, is central to all of The UM - Missoula's business goals, requirements, and operations. CIS controls the network, including managing central equipment and operation. However, security for some aspects of the network is distributed among CIS and business process owners, because The UM - Missoula business process owners control and administer hardware, such as servers and desktops, residing on the network.

Audit Objectives

We performed audit work on The UM - Missoula campus to meet the following three objectives:

1. To provide assurances over key Banner application controls identified by Legislative Audit Division Financial-Compliance audit staff. Control objectives were specific to the human resource, student financial aid, and finance modules. A technical memorandum has been provided to the audit staff for consideration during financial audits.

2. To evaluate the general controls environment where the Banner application resides. Control objectives were to provide reasonable assurance that controls exist over the Banner system software, hardware, and data to ensure they are protected from unauthorized or unnecessary access and environmental factors.

3. To review the security administration over the network environment and assess the security of selected workstations

residing on the network. Control objectives were to provide reasonable assurance that controls exist over the network and workstations to maintain a minimum level of security.

Audit Scope and Methodology

The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office. We evaluated the control environment using information security best practices, Control Objectives for Information and Technology (COBIT), computer security incident response team CERT®, SANS Institute, A Security Checklist for Oracle9i, and the Board of Regents Policy for Security of Data and Information Technology Resources.

We audit selected The UM Banner processes approximately every two years to understand the control environment. The current audit scope is based on specific control testing requested by Financial-Compliance staff and specific general controls testing determined relevant to the Banner application.

We reviewed key Banner application controls over human resources, finance and student financial aid. We tested and concluded on the following key controls:

- We determined the payroll deduction rates and leave accrual rates residing in underlying system tables contain appropriate rates consistent with the current year governing federal or state law, and the activity date is consistent with the applicable rate effective date.
- For specific automated student financial aid forms, we determined procedures are in place to limit system access and input functions to current employees.
- We determined procedures are in place to ensure the information exchange with the Department of Education on student aid data is complete and the process is controlled.
- We determined that the cost of attendance amounts residing in Banner are consistent with the rates developed by the Financial Aid Office, and reflect the most current academic year budgets.

- We determined the programming used to assign satisfactory academic progress operates according to management's description and understanding.
- We determined access to automated forms used to reduce or adjust student accounts receivables was limited to appropriate individuals currently employed by The UM.
- We determined valid transactions from the legacy system files are accepted for processing by the finance module.
- We determined documents failing to post in an accounting period are appropriately captured and rolled forward to the next period.
- Since ultimately Banner information is exchanged with the Statewide Accounting, Budgeting and Human Resource System (SABHRS), we determined the interface process identifies Banner information to upload to SABHRS and translates account elements accordingly.

General controls testing was limited to The UM - Missoula's Banner application and its respective operating environment. Through the use of automated tools, interviews with The UM - Missoula management and staff, and observation of physical and environmental controls, we evaluated the overall security of the Banner environment. Weak security controls on any aspect of The UM - Missoula network could potentially affect the availability of the network and, thus, the availability of the Banner application. We performed a review of the security administration over the network and selected workstations, based on the operator's access to Banner and ability to perform adjustments to Banner data, and tested the workstations to determine if adequate security existed for maintaining a minimum level of security.

Management Memo

During the course of our audit, we identified two issues that warranted management attention, but were not included as recommendations in this report. We identified the following issues and communicated them to The UM - Missoula through a management memo:

- Undocumented controls over the financial aid user access authorization process and the process to monitor user access
- Services available for use on a financial aid workstation which were unnecessary for the intended use of the workstation

Chapter II - Physical Security

Introduction

Physical security encompasses both the equipment location and the condition of the location. Physical security involves restricting physical access to computer resources, usually by limiting access to the buildings and rooms where they are housed and protecting against environmental factors by preventing or mitigating potential damage to the location and interruptions in service from fire, water leaks, or smoke. Physical security controls protect computer resources from intentional or unintentional loss or impairment.

Conclusion

Based on our work, controls exist to ensure Banner hardware, software, and data are safeguarded. The UM - Missoula management can improve security by addressing inadequate environmental controls and excessive physical access to the computer facility housing Banner backup and network equipment.

Inadequate Environmental Controls

The UM - Missoula has established a computer facility as a Banner backup and network site. Banner production data is copied and stored on the Banner backup hardware residing in this site. In the event that the computer facility housing the Banner production data and equipment is unavailable, the backup Banner equipment and data would be established as Banner production for business continuity. Within the facility, the university also houses campus network equipment. All inbound electronic communications to the campus and all outbound electronic communication from the campus arrive and depart using the network equipment, including communication with the Internet and SummitNet, the State of Montana's data communications network. The UM - Missoula uses SummitNet to transmit Banner data to the Statewide Accounting, Budgeting and Human Resource System (SABHRS).

We examined the physical and environmental controls over The UM - Missoula computer facility. As illustrated in Figures 1 through 4, we identified computer equipment, power cords and power cables sitting directly on the floor, susceptible to water damage. There are water and sewer pipes, open running water, and exposed flexible water lines to movable cooling devices. Damage to water lines and pipes or misalignment of the open water source could lead to water

drainage and water accumulation. Water accumulation could damage equipment and disrupt Banner backup availability and network services disabling The UM - Missoula's ability to electronically send or receive communication external to the campus, including the transmission of Banner data to SABHRS.

Figure 1

Open Running Water Located near Banner Backup and Network Equipment

Source: Photo by Legislative Audit Division

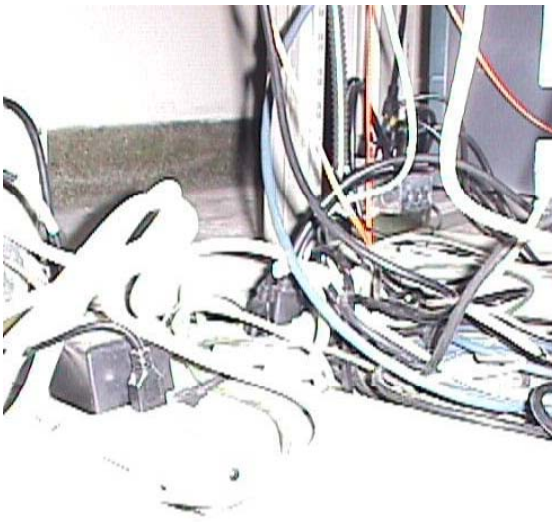
Figure 2

Water and Sewer Pipes Above Banner Oracle Data Servers

Source: Photo by Legislative Audit Division

Figure 3

Power Cords and Cables to Network Equipment Located Directly on Floor



Source: Photo by Legislative Audit Division

Figure 4

Proper Cabling within The UM - Missoula's computer facility housing Banner production equipment, illustrating organized power cords and cables and elevation from the floor.

Source: Photo by Legislative Audit Division

Chapter II - Physical Security

Industry standards recommend sufficient measures be in place and maintained for protection against environmental factors. Physical security of the computer facility housing the Banner backup and network equipment has not been a priority of The UM - Missoula management. The UM - Missoula personnel stated the risk created by water pipes can be reduced by spending $10,000 to $12,000 on raised floors and a power distribution unit to partially mitigate damage to approximately $500,000 worth of equipment. According to personnel, these steps have not been taken due to budgeting and available funds.

Recommendation #1

We recommend The UM - Missoula evaluate environmental conditions in the computer facility and make necessary changes.

Excessive Physical Access

The computer facility housing the Banner backup equipment is divided into four rooms. The first room is an office and storage area and does not contain any computer equipment, the second room contains the network equipment, the third room contains the Banner backup equipment, and the fourth room contains plumbing system fixtures. Physical access to rooms two, three and four is gained through room one. We identified 91 individuals with physical access to the network equipment and 84 individuals with physical access to the Banner backup equipment. Eighteen of these individuals are members of the CIS department and need access to these rooms for information technology reasons. The remaining 66 individuals have access for reasons not related to information technology, such as required physical access to a mechanical room only accessible through the equipment rooms. Therefore, access to Banner and network equipment and services is available to individuals who do not need the access to perform their jobs.

Physical security involves limiting access to computer hardware, wiring, and network devices to prevent accidents, damage, or tampering of physical hardware. Industry standards recommend

implementing appropriate physical access controls to prevent theft or destruction, such as surveillance cameras or escort of individuals who are not members of the information technology group by a member of the information technology group when entering computer facilities.

Given the physical condition of the rooms (cables, pipes, etc.), the more people with access to these rooms the greater the likelihood of service disruption by intentional or unintentional contact with equipment, power cables and water pipes.

Card readers control physical access to rooms one, two, and three with entry being logged by the card reader software. However, the access log is not consistently reviewed and only addresses who has entered the rooms, not activities performed while in the rooms.

Recommendation #2

We recommend The UM - Missoula evaluate the number of individuals with physical access to the computer facility and ensure appropriate physical access controls.

Chapter III - Network Security

Information Technology Organization Structure

The UM - Missoula information technology environment is complex with many areas of responsibility for administration of information technology resources. The Chief Information Officer (CIO) of the CIS department "owns" the network. CIS manages the equipment, operates the network, and administers the Banner application. However, business process owners can also control aspects of the network via devices attached to the network such as applications, servers, and workstations. The network and its security provide the foundation for all systems and software applications. It is central to all of The UM - Missoula's business goals, requirements, and operations.

Conclusion

Based on our work, controls exist to ensure Banner hardware, software, and data are safeguarded. However, because there is no single focus on network security, and there are devices connected to the network for which the security administration is not controlled by CIS, The UM - Missoula can improve security by complying with Board of Regents policy to identify security issues and exposures and develop policies to mitigate those concerns, and designate an information security manager.

Distributed Network Security Administration

Under the Montana Board of Regents policy, each campus of the Montana University System is required to establish and maintain policies for the security of data and information technology resources. Board of Regents policy states that The UM - Missoula chief executive officer shall assign to appropriate individuals or groups the responsibility for development of policies governing the security of data and information technology resources that specifically encompass the responsibilities outlined in state law, section 2-15-114, MCA, including, but not limited to, designating an information security manager.

According to The UM - Missoula CIO, The UM - Missoula does not have an information security manager. During the current audit, we determined The UM - Missoula information technology environment has no single focus on network security. There are multiple parties

responsible for performing security related activities and because of the diffused responsibilities, no one individual or group has taken or been given the responsibility to manage network security. There is no clearly documented responsibility lines or boundaries between the CIS department and The UM - Missoula business process owners. Therefore, when we asked for information on server locations, patch management policies, disaster recovery efforts, and computer addresses residing on the network, our requests were difficult for CIS to meet and the information could not be provided that addressed the entire campus. CIS provides services such as e-mail, virus protection, and software update services, however business process owners have the choice to "opt-in" to these services. The UM - Missoula business process owners can use services offered by CIS, operate their own services, or choose not to use any services. Consequently, there are locations on-campus over which CIS has no control, even though the administration of security at those locations may impact the network.

Workstation Vulnerabilities

Workstations are an access point to The UM - Missoula network and the Banner application. Workstations with inappropriate or unnecessary services available create vulnerabilities and provide opportunities for a knowledgeable person to gain system access to sensitive information. From three non-CIS departments we selected 45 workstations based on the operator's access to Banner and ability to perform adjustments to Banner data. We tested these workstations for services having commonly known vulnerabilities and discussed the following results with department staff:

- *Anonymous Login*: 22 of 45 workstations tested provided an unnecessary ability to view user account detail. The UM - Missoula's operating system has a built-in function that allows anonymous connection by default. An anonymous connection is where a computer can connect to another without providing a password or username. This connection can be used to display sensitive information such as user account information, which can be used to gain access to data stored on that workstation. Two higher levels of security are available. Level one restricts

access to user account information and level two denies anonymous connections requiring all computers to provide credentials.

- *Administrator Account*: 12 of 45 workstations tested maintained default configuration settings. The UM - Missoula's operating system default configuration includes an administrator account named "Administrator," which is associated with local workstation services. The administrator account has full control over the computer and is the only account that is automatically granted every built-in right and ability in the system. The default administrator account, "Administrator," is well known in the intruder community and is often times a target for intruders because it is easier to use the default administrator account name than guessing the names of other accounts that have permissions equal to the administrator account.

- *Security Updates*: All 45 workstations tested were current with the critical security updates released by The UM - Missoula's operating system vendor. Each of the three departments tested have opted to participate in CIS's security update service. Security updates are released by vendors and are corrections to security related problems in software systems. Workstations which are not current with security updates create vulnerabilities for service disruption creating risk to the entire network. For example, as reported by The UM - Missoula in the fall of 2003, several e-mail based viruses were released on the Internet. Students and faculty returning from summer break had workstations with out-of-date security and virus protection and thus, were not appropriately secured from the newly released viruses. The viruses were able to enter The UM - Missoula network and consequently The UM - Missoula had to temporarily disconnect major portions of the campus network to keep the virus from bringing the entire network to a halt.

Board of Regents policy states that the chief executive officer shall assign appropriate individuals or groups to engage in the

identification of security issues and exposures and shall develop draft policies reflecting those concerns. Our testing results showed that the business process administrators had identified workstation security issues. However, because The UM - Missoula has not identified security issues and exposures and developed policies to reflect those concerns, each administrator has a different idea of what should be considered a workstation vulnerability. For example, one administrator has identified the default account name "Administrator" as a vulnerability; however, the other two business process administrators did not consider this a security issue. Although business process administrators were addressing workstation security vulnerabilities, each have varying ideas on what a workstation vulnerability is; workstation security is not consistently applied.

Recommendation #3

We recommend The UM - Missoula comply with Board of Regents policy and:

A. Designate an information security manager; and

B. Assign individuals or groups to engage in the identification of security issues and exposures and develop policies mitigating those concerns.

University Response

The University of Montana

Office of the President
The University of Montana
Missoula, Montana 59812-3324
Office: (406) 243-2311
FAX: (406) 243-2797

22 July 2004

Mr. Scott A. Seacat
Legislative Auditor
Legislative Audit Division
Room 135 State Capitol
P. O. Box 201705
Helena, MT 59620-1705

Dear Mr. Seacat:

We compliment the Legislative Audit staff for their cooperation and completion of The University of Montana-Missoula's Key Computer Application and General Control Audit. The University concurs with the recommendations made and presents our plan to address the areas of concern.

We appreciate the cooperative efforts made by the audit team and thank those involved for their assistance. Also, we remain committed to reliable systems of control and accountability for The University of Montana.

Sincerely,

George M. Dennison
President

Enclosure

c: R. Duringer, Vice President for Administration and Finance
S. Stearns, Commissioner of Higher Education

GMD/ab
denlet2808

The University of Montana - Missoula

Response to Legislative Audit Division
Key Computer Application and General Control Audit
July 2004

RECOMMENDATION #1
WE RECOMMEND THE UM-MISSOULA EVALUATE ENVIRONMENTAL CONDITIONS IN THE COMPUTER FACILITY AND MAKE NECESSARY CHANGES.

The University concurs with the recommendation. University personnel will develop a plan to address the noted environmental weaknesses in our backup facilities by 1 November 2004. With the estimated cost known by 1 November, the plan will be completed in fiscal year 2005 or 2006 depending on the funds needed.

RECOMMENDATION #2
WE RECOMMEND THE UM-MISSOULA EVALUATE THE NUMBER OF INDIVIDUALS WITH PHYSICAL ACCESS TO THE COMPUTER FACILITY AND ENSURE APPROPRIATE PHYSICAL ACCESS CONTROL.

The University concurs with the recommendation. In reconfiguring space for Recommendation 1, University personnel will also address the physical access weaknesses noted. During the remodeling of the backup facility, University personnel will review individual physical access and limit that access where appropriate by job duties.

RECOMMENDATION #3
WE RECOMMEND THE UM-MISSOULA COMPLY WITH BOARD OF REGENT POLICY AND:

A: DESIGNATE AN INFORMATION SECURITY MANAGER; AND
B: ASSIGN INDIVIDUALS OR GROUPS TO ENGAGE IN THE IDENTIFICATION OF SECURITY ISSUES AND EXPOSURES AND DEVELOP POLICIES MITIGATING THOSE CONCERNS.

The University concurs with the recommendation. The University President will designate the Associate Vice President for Information Technology to draft policies to conform to BOR policy 1300.1. Starting in Fall 2004, the drafted policies will be reviewed by the various campus constituents with final adoption and OCHE approval by 30 June 2005.

Existing University personnel will be utilized to develop the policies. Once the policies and standards have been adopted the designation of an information security manager will follow. However, we anticipate enforcement of those policies may require additional personnel. The cost estimate for the compliance/enforcement personnel is $75,000 - $110,000.